(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－162601
（P2003－162601A）
(43)公開日　平成15年６月６日(2003.6.6)

(51)Int.Cl.'		識別記号	FI			テーマコード'（参考）
G06F	17/60	142	G06F	17/60	142	5B017
		302			302E	5B085
	12/14	320		12/14	320A	
	15/00	330		15/00	330Z	

審査請求　未請求　請求項の数１　ＯＬ　（全 8 頁）

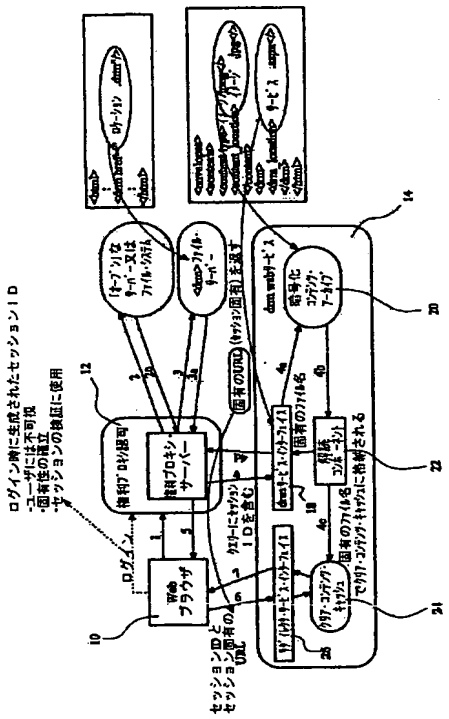
(21)出願番号　特願2002－237927(P2002－237927)
(22)出願日　平成14年８月19日(2002.8.19)
(31)優先権主張番号　０９／９４１，６１５
(32)優先日　平成13年８月30日(2001.8.30)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　ジョン・エス・エリクソン
アメリカ合衆国05055バーモント州ノーウィッチ、132・ルート　707
(74)代理人　100081721
弁理士　岡田　次生　（外２名）

最終頁に続く

(54)【発明の名称】　プロキシ・サービス提供装置

(57)【要約】
【課題】クライアント・プラットフォームと電子的なコンテンツを提供するリモート・コンテンツ・プロバイダの間のプロキシ・サービスを提供する装置を提供する。
【解決手段】の装置は、コンテンツ・プロバイダの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈する手段と、前記要求をコンテンツ・プロバイダに送信し、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも１つのマーカーを含むデータを受け取る手段と、前記１つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信する手段を備えている。



1

【特許請求の範囲】

【請求項１】１つ又は複数のクライアント・プラットフォームと１つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置であって、

（ａ）リモート・プラットフォームの電子的なコンテンツ又は情報に対するクライアント・プラットフォームの要求を受信し解釈し、前記要求を前記リモート・プラットフォームに送信し、データを受け取る機能、または

（ｂ）前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォームから受け取る機能のいずれか又は両方を行う手段を備え、

前記データは、要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービスのロケーションを表す少なくとも１つのマーカーを含んでおり、

前記装置は、前記１つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、

（ａ）前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能、または

（ｂ）前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、

を備えるよう構成されたプロキシ・サービス提供装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一般に電子権利管理に関し、特に情報技術ネットワーク環境専用の権利管理方式や他の情報操作ポリシーをサポートする柔軟なプラットフォームに関する。

【０００２】

【従来の技術】著作権は特定の種類の作品の原作者に与えられる知的所有権であり、原作者は著作権によってその作品の様々な利用法を管理できる。著作権は、文学、戯曲、音楽、美術の作品、出版物、録音物、映画（ビデオを含む）、放送（有線放送、衛星放送を含む）の原作を保護するためのものであり、著作権によって提供される権利は、保護の対象となる作品の複製、翻案、複製の配布、公演、放送などの様々な領域に及ぶ。また、多くの場合、著者には自分の作品であることを特定される権利と、自分の作品の毀損や変形に異議を唱える権利がある。さらに、録音物、映画、コンピュータ・プログラムの著作権所有者には貸与の権利が与えられるので、このような作品を公に貸し出すことによって実施するには著作権所有者から交付されたライセンスが必要になる。

【０００３】近年、録音物、文学作品、映画などのコンテンツの電子的な保存がますます一般的になってきており、レコード店や書店などの小売店ではこのような電子コンテンツの商品流通が従来から行われている。情報技術ネットワークを介した電子コンテンツの商品流通には多くの利点があるが、このようなコンテンツの作者や流通業者に広く採用されているわけではない。その主な理由は、結果としてこのようなコンテンツをサード・パーティーが不法に複製、販売、配布しやすくなるのではないかという懸念である。このために、電子コンテンツの不当な複製を防止する技術的な防護策の開発に向けて多大な努力が払われてきた。

2

【０００４】デジタル・コンテンツは不法な複製が比較的容易であり、このことがコンテンツ・プロバイダにとっては好都合でもあり、不都合でもある。すなわち一方でコンテンツをできるだけ広く配布できるのは望ましいが（それによって価値が高まり、大きな利益の獲得も見込まれる）、依然として販売ごとに確実に支払いがあること、つまり著作権が侵害されないことを望んでいる。前述のような著作権侵害を防止するために、コンテンツ・プロバイダはデジタル保護方式（通常は暗号化技術に基づく）を採用する傾向がある。この方式は、ａ）消費者には使いにくく配布の制限が難しい、ｂ）　管理に費用がかかる、ｃ）同等のコンテンツをユーザーが操作しやすい無料の不法な方式によって無効化される恐れがある。

【０００５】既知の保護方式の１つはＭｉｃｒｏｓｏｆｔ　Ｄｉｇｉｔａｌ　ＭｅｄｉａＳｙｓｔｅｍから提供されており、電子コンテンツがキーを伴って提供される。ユーザーは、正規のキー・サーバーから対応するキーを取得しないとコンテンツを再生できない。この方式の主な欠点は、ユーザーの再生装置との結び付きが強いことである。つまり、この方式で保護されたコンテンツを再生する場合は、専用の装置が必要になる。

【０００６】一般に、既知のデジタル権利管理及び保護方式には、作品の実質的な暗号化が含まれており、複製や複製されたコンテンツの再生が難しくなっている。現在使用されているデジタル権利管理（ＤＲＭ：Ｄｉｇｉｔａｌ　ｒｉｇｈｔｓ　ｍａｎａｇｅｍｅｎｔ）技術は、ユーザーにはセキュア・コンテナとしても知られている。すなわち、この技術によって独自のファイル・フォーマットを定義し、その中で任意のメディア・ファイルをセキュアにカプセル化する。

【０００７】例えば、米国特許第６１３８１１９号に権利管理データ構造を定義、利用、操作するための技術が示されている。この明細書では、セキュアなデジタル・コンテナの概念を使用してデジタル・コンテンツの安全でセキュアな保存と転送を実現している。このようなコンテナは改ざんが難しいので、例えば、テキスト、グラフィック、実行可能ソフトウェア、オーディオやビデオなど、任意の形式のデジタル情報をパッケージ化するの

に利用できる。ただし、この方法ではセキュアなコンテンツを利用できる状況が限定される。

【０００８】別のシステムでは、特定のメディア・フォーマット（Ａｄｏｂｅ（商標）　ＰＤＦなど）に対して「プラグイン」セキュリティ機能を提供する。ソフトウェア・プラグイン・ビジネス・モデルは、ビデオやオーディオ（接続可能なｃｏｄｅｃ）、マルチメディア（プログラムを「拡張」する接続可能な実行プログラム）、クリエイティビティ・ツール（画像処理ツールを拡張するフィルタ）、Ｗｅｂブラウザなど、他の特定の市場で長年にわたってアプリケーションの拡張に使用されてきたが、現在ではＡｄｏｂｅ　Ａｃｒｏｂａｔ　（商標）のみがセキュリティ機能を提供しており、サード・パーティーの開発者はＡｃｒｏｂａｔ　ＴＭを使用して特定のフォーマットで機能するＤＲＭを一律に開発できる。ただし、このシステムで使用する方法は、ターゲット・フォーマット（ＰＤＦ）の機能によって制限される。つまり、この方法ではセキュリティを保証できるフォーマットが一種類に限定され、メディアの種類が限定される。

【０００９】デジタル情報製品のプロバイダ、仲介業者、消費者は、情報製作者が知的所有権（ＩＰＲ）を提示し、ＩＰＲポリシー（特に卸売業者、小売業者、ライブラリなどの仲介業者が情報を操作する規則を表すポリシー）を主張する一貫したプラットフォームのない「ポリシー実施の断片化」に悩まされている。このような情報をユーザー向けに表示し、ポリシーを解釈して実施するための一貫したプラットフォームは存在しない。ネットワーク・トランザクションの途中で公表できる私的なデータの送信と再利用に関わる消費者も、やはり一貫したプラットフォームを用意してその制御下で個人的な情報を操作するポリシーを実施しているわけではない。

【００１０】一般に、情報バリュー・チェーンに関わるユーザーは、操作する情報の取扱いについて要求するポリシーと受け取った情報の取扱い又は処理についてのポリシーを提示してから情報を受け取ることを希望している。既知の技術では、この問題を一貫した体系的な方法で解決することはできない。

【００１１】コンテンツのフィルタリングと適応のためにプロキシ・サービスを利用するという概念が知られている（「プロキシ」は、広義では単に「代理に付与された権限」を意味する）。例えば、望ましくないコンテンツの広告などを除去するための規則に基づくフィルタリングは、新たに発生した作業である。特に米国特許第５，９９６，０１１号では、ネットワークを介してコンピュータが受け取るデータから特定のデータをフィルタで除去することによって、受け取ったデータへのアクセスを制限するシステム及び方法について記述している。１つの実施態様では、インターネットに接続されたコンピュータが受け取るＷｏｒｌｄ　ＷｉｄｅＷｅｂページから好ましくないテキスト・データ又は対象となるテキスト・データをフィルタリングするコンピュータベースの方法が示されている。米国特許第６，１１９，１６５号には、インターネット又はインターネット環境において、多くのクライアントをサポートするプロキシ・サーバーに機能を追加し、クライアントの特性に基づいて特定のクライアントにソフトウェア・モジュールを提供できるようにするシステムに関する記述がある。こうしてダウンロードされたモジュールは、プロキシ・サーバーとクライアントとの双方向通信リンクをセットアップしたクライアントによって実行される。双方向リンクによって、例えばクライアント・プラットフォームのウィンドウを使用したクライアント側でのステータス表示が可能になり、ウィルス・スキャン、コンテンツのフィルタリング、帯域幅利用など、プロキシ・サーバーの現在のステータスを表示できる。他のアプリケーションでは、ダウンロードされたモジュールによって組織の掲示板、ニュース・チャネル、一般的なソフトウェア・パッチの提供元を構築できる。

【００１２】米国特許第５，９８７，６０６号には、インターネット・コンピュータ・ネットワークからリモート・インターネット・サービス・プロバイダのサーバーによって取得され、ローカル・クライアント・コンピュータに転送されるインターネット・コンテンツをフィルタリングするシステムが示されている。このシステムでは、包含的なフィルタや排他的なフィルタなどの少なくとも１つのフィルタリング方式と、許可されるサイト又は除外されるサイトのリストなどの少なくとも１つのフィルタリング要素をローカル・クライアント・コンピュータで生成された個々のインターネット要求と照合する。この場合はＩＳＰサーバーにフィルタリング方式が実装されているが、一般にこの種のフィルタリング・サービスや適応サービスはクライアント側、サーバー、両者の中間点のいずれに適用してもよい。さらに、フィルタリングと適応はダウンストリーム・コンテンツ（クライアント・プラットフォームがサーバーから受け取るコンテンツ）に限定する必要はない。つまり、プライバシーや匿名を保証するためにユーザー入力に適応するプロキシ・サービスが存在する。

【００１３】

【発明が解決しようとする課題】ただし、既知のプロキシ・サービスはいずれも情報操作ポリシーの適用（特に著作権の管理と行使のサービス）の実際的な介入ポイントを提供しない。前述のとおり、一般に著作権ポリシーを実施する既知のメカニズムでは、通常クライエント側で特別な「読み出し」ソフトウェアを使用し、コンテンツに関するエンドユーザーの楽しみを損なう結果になるか、サーバー側で非常に限定的なコンテンツに依存するポリシー実施機能を使用し、エンドユーザが鑑賞できるコンテンツを制限してしまうことになる。専用のクライ

アント・アプリケーションには、プラットフォーム互換性やアプリケーション互換性による制限からユーザーの不便まで、多くの欠点がある。既知のサーバーベースのシステムにも、管理上の粒状性の問題からコンテンツの柔軟性の問題まで、多くの弱点がある。

【００１４】

【課題を解決するための手段】そこで、以上の問題を克服するための仕組みを考案した。こうして、本発明の第１の側面に従って、１つ又は複数のクライアント・プラットフォームと電子的なコンテンツ又は情報を提供する１つ又は複数のリモート・コンテンツ・プロバイダの間のプロキシ・サービスを提供する装置が提供される。

【００１５】この装置は、コンテンツ・プロバイダの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈する手段と、前記要求をコンテンツ・プロバイダに送信し、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも１つのマーカーを含むデータを受け取る手段と、前記１つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信する手段を備えている。

【００１６】また、本発明の第１の側面に従って、１つ又は複数のクライアント・プラットフォームと電子コンテンツを提供する１つ又は複数のリモート・コンテンツ・サーバーの間のプロキシ・サービスを提供する方法も提供される。本方法には、コンテンツ・サーバーの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈するステップと、前記要求をコンテンツ・サーバーに送信するステップと、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも１つのマーカーを含むデータを受け取るステップと、前記１つ又は複数のマーカーを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信するステップが含まれる。

【００１７】本発明の第２の側面に従って、１つ又は複数のクライアント・プラットフォームと前記１つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された１つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置が提供される。本装置は、リモート・プラットフォームに送信するデータが前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも１つのマーカーを含んでいる場合に、前記データをクライアント・プラットフォームから受け取る手段と、前記１つ又は複数のマーカーを解釈する手段と、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する手段を備えている。

【００１８】さらに、本発明の第２の側面に従って、１つ又は複数のクライアント・プラットフォームと前記１つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された１つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する方法も提供される。本方法には、リモート・プラットフォームに送信するデータがリモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも１つのマーカーを含む場合に、前記データをクライアント・プラットフォームから受け取るステップと、前記１つ又は複数のマーカーを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信するステップが含まれる。

【００１９】このようにして、本発明はクライアント・プラットフォームと様々な権利管理ポリシーや情報操作ポリシーを伴う様々なコンテンツ・プロバイダとの中継点として利用できるプロキシ・サービスを提供し、それによってコンテンツ・プロバイダは自社の独自のポリシーを確実に実施できる。従って、本発明はクライアント・プラットフォームとクライアント・プラットフォームが機密性の高い情報や個人的な情報を送信する様々なリモート・ロケーションとの中継点として利用できるプロキシ・サービスを提供し、それによってクライアント・プラットフォームの機密性／匿名性に関する独自のポリシーを確実に維持できる。本発明に従った１つのプロキシ・サービスは２つの目的で利用できる。つまり、このようなサービスはクライアント・プラットフォームから受信するデータとクライアント・プラットフォームに送信するデータの両方を処理するように調整できる。

【００２０】本プロキシ・サービスは、クライアント・プラットフォーム上にローカルに配置してもよい。ただし、「クライアント」が複数のプラットフォームを含む組織的なネットワークを備える場合は、本プロキシ・サービスをそのネットワーク内の中心に配置してもよい。あるいは、本プロキシ・サーバーをインターネットなどの情報技術ネットワークのリモート・ポイントに配置してもよい。

【００２１】コンテンツ・サーバーは、本プロキシ・サービスからのコンテンツ要求に応答して１つ又は複数のマーカーを含むデータ・ストリームを返す。マーカーには、プロキシ・サービスがクライアント・プラットフォームにコンテンツの複製を送信する前に対話する必要がある他の１つ又は複数のサービスのロケーションの詳細情報（ＵＲＬやＤＯＩなど）が含まれる。このようなマーカーはデータ・ストリームに埋め込まれており、これを認識でき、解釈できるのはプロキシ・サービスの内部で提供される専用の手段に限定されるのが好ましい。

【００２２】クライアント・プラットフォームがＷｅｂブラウザなどの場合は、情報操作／権利管理リモート・サーバーにコンテンツ要求を送信する際に（直接又は間接的に）、プロキシ・サービスは要求内にクライアント・プラットフォームに関連するデータ（セッションＩＤなど）を含むように調整されているのが好ましい。従って、情報操作／権利管理リモート・サーバーにクライアント・プラットフォームに関する情報が提供される。要求には、エンド・ユーザーに固有の詳細情報を含めることもできる（特に、エンド・ユーザーとクライアント・プラットフォームが別のエンティティであり、エンド・ユーザーとクライアント・プラットフォームが対話するための情報操作／権利管理サーバーに関連する特別な要件がない場合）。

【００２３】情報操作／権利管理サーバーがプロキシ・サービスからコンテンツ要求を受信し、要求の合法性を検証すると、情報操作／権利管理サーバーはコンテンツのクリア・コンテンツ・バージョンを作成し、これをローカル又はリモートの特定のロケーションに保存し（できれば一時的に）、さらに前記ロケーションの詳細情報をプロキシ・サービスに返す。プロキシ・サービスは、コンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォームのロケーションの詳細情報を送信するように調整できるのが好ましい。このことによって、情報操作／権利管理サーバーに関する特定の要件が満足された場合に、クライアント・プラットフォームは前記クリア・コンテンツの複製を取得できる。

【００２４】情報操作／権利管理サーバーが採用するポリシーがコンテンツ・プロバイダと（当然のことながら）要求されたコンテンツの性質に依存するのは言うまでもない。情報操作／権利管理サービスがクライアント・プラットフォーム又はエンド・ユーザーに関連付けできることも明らかである。このことによって、クライアント・プラットフォームからリモート・ロケーションに送信される情報をプロキシ・サーバーによって操作し、適切な情報操作サービスを介して処理してから、前記リモート・ロケーションに送信できる。

【００２５】

【発明の実施の形態】ここで、単に例として添付の図面

を参照しながら本発明の１つの実施態様について説明する。

【００２６】図１を参照すると、Ｗｅｂブラウザ１０（クライアント・コンピュータ・プラットフォーム（図示せず）からアクセス可能）、本発明に従ったプロキシ・サーバー１２、デジタル権利管理（ＤＲＭ）Ｗｅｂサービス１４の間の典型的な接続（１つの例）が示されている。この接続は、通常はインターネットなどの情報技術ネットワークを介して行われる。矢印１、２、２ａ、３、３ａ、４、４ａ、４ｂ、４ｃ、４ｄ、５、６、７は、以下に記述する典型的なプロセスでＷｅｂブラウザ１０、プロキシ・サーバー１２、ＤＲＭ　Ｗｅｂサービス１４の間でやりとりする要求や応答の方向を示している。

【００２７】最初のインスタンスでは、固有のセッションＩＤが生成された時点でＷｅｂブラウザ１０がプロキシ・サーバー１２にログインする。セッションＩＤはエンド・ユーザーには認識されず、後のプロセスでセッションの検証に使用される。

【００２８】矢印１を参照すると、表示側クライアントすなわちＷｅｂブラウザ１０はプロキシ・サーバー１２にネットワーク・アドレス（例えばＵＲＬやＤＯＩ）を提示することでネットワーク・リソースの要求を行う。プロキシ・サーバー１２は、ユーザーのワークステーションにローカルにも、企業や組織のネットワークに集中的にも、あるいはインターネットなどの情報技術ネットワークのリモート・ポイントにも配置できるのは言うまでもない。

【００２９】プロキシ・サーバー１２は、通常は、ＨＴＴＰプロトコルを使用して、コンテンツ・サーバー１６にリソースへの適切なネットワーク要求を送信する（矢印２）。コンテンツ・サーバー１６は、通常はプロキシ・サーバー１２とは別のロケーションに存在し、Ｗｅｂページなどのリソースを返す（矢印２ａ）。リソースは、一般にＨＴＭＬファイル又はより一般的なＸＭＬファイルの形式をとる。リソース・ファイルには、他のリソースを呼び出すマークアップ・タグに類するものが埋め込まれており、プロキシ・サーバー１２が提供する情報操作ポリシー又はデジタル権利管理に従った専用の処理のみによって取得できる。本発明のこの実施態様では、この種のマークアップ・タグは＜ＤＲＭ＞オブジェクトとして記述される。プロキシ・サーバー１２に送信される他の「オープン」なデータ・ストリーム内のこのような＜ＤＲＭ＞オブジェクト・インスタンスは、プロキシ・サーバー１２が埋め込みコンテンツ・オブジェクトのクリア（すなわち暗号化されていない）バージョンのロケーションを確認するために対話する必要のある他のＷｅｂリソースを参照する属性（ＵＲＬやＤＯＩなど）を備えている。

【００３０】コンテンツ・サーバー１６から受け取った

データ・ストリーム内に埋め込まれたマークアップ・タグにプロキシ・サーバー１２が適応するのは言うまでもない。最初にプロキシ・サーバー１２を通過することなくＷｅｂブラウザ１０がコンテンツ・サーバー１６から直接データ・ストリームを取得しようとしても、ブラウザが認識できるのはストリームの「オープン」な部分のみである。従って、マークアップ・タグを認識も解釈もできない（つまりＷｅｂブラウザ１０はタグを無視する）。

【００３１】プロキシ・サーバー１２はコンテンツ・サーバー１６からリソース・データ・ストリームを受け取ると、生成された一連の規則に従って受信したストリームを確認し、データ・ストリームに埋め込まれた１つ又は複数のマークアップ・タグを検出する。プロキシ・サーバー１２は、例えばインターネット上のリモート・ポイントに配置された「ｄｒｍファイル」のロケーションを示すプロパティをタグ本文から抽出するように調整されている。次に、プロキシ・サーバー１２は指定された＜ＤＲＭ＞ファイル（１つ以上）を要求し（矢印３）、受信する（矢印３ａ）。＜ＤＲＭ＞ファイルでは、例えばＸＭＬ構文を使用してもよい。プロキシ・サーバー１２は、このファイルから実際のコンテンツ・オブジェクト（通常はセキュア・コンテナなどにパッケージ化されている）の”ｃｏｎｔｅｎｔ＿ｔｙｐｅ”と”ｃｏｎｔｅｎｔ＿ｌｏｃａｔｉｏｎ”（例えばＵＲＬ）を抽出する。

【００３２】このサービスは、通常は”ＭＩＭＥ”エンコード（ｉｍａｇｅ／ｊｐｅｇなど）を使用したｃｏｎｔｅｎｔ＿ｔｙｐｅを解釈し、このｃｏｎｔｅｎｔ＿ｔｙｐｅをプロキシ・サービスに登録した１つ又は複数のｃｏｎｔｅｎｔ＿ｔｙｐｅと比較する。ｃｏｎｔｅｎｔ＿ｔｙｐｅがサービスに登録されたタイプの１つであれば、エンド・ユーザーに返す「クリア」なタグ構造が決定する。例えば、パッケージ化されたコンテンツがＭＩＭＥタイプ・イメージ／ｊｐｅｇの場合、変更されたタグ構造は”＜ｉｍｇ　ｓｒｃ＝’．．．’＞”のフォーマットでなければならない。つまり、エンド・ユーザーが（例えば登録ユーザーやライセンスを付与されたユーザーとして）リソースを使用できるようにする場合、プロキシ・サーバー１２は次のように動作する。

【００３３】ここで、プロキシ・サーバー１２は、リモートＤＲＭ　Ｗｅｂサービス１４が指定されたリソースのセッションに固有の「クリアコンテンツ」バージョンを作成し、セッションに固有のＵＲＬを返すことを要求する（矢印４）。詳しく記述すると、ｄｒｍサービス・インターフェイス１８は＜ｄｒｍ＞ファイルの暗号化バージョンをｄｒｍ　Ｗｅｂサービス１４内の暗号化コンテンツ・アーカイブ２０に配置する（矢印４ａ）。次に、コンテンツ・アーカイブ２０は暗号化された＜ｄｒｍ＞ファイルを、やはりｄｒｍ　Ｗｅｂサービス１４内に存在する解読コンポーネント２２に送信する。解読コンポーネント２２は、ファイルを解読してその「クリアコンテンツ」バージョンを作成する。このクリアコンテンツ・バージョンは、セッションに固有の（一時的な）固有のファイル名を使用して、やはりｄｒｍ　Ｗｅｂサービス１４内に存在するクリアコンテンツ・キャッシュ２４に送信され（矢印４ｃ）、キャッシングされる。また、固有のファイル名はｄｒｍサービス・インターフェイス１８に送信され、セキュアでないリソースのセッション固有のＵＲＬを生成してプロキシ・サーバー１２に送信する（矢印４ｄ）。

【００３４】プロキシ・サーバー１２は、（この場合は）ＭＩＭＥ対応のフォーマットを使用して変更されたコンテンツ・ストリーム（例えばＨＴＭＬページ）を作成する。ＨＴＭＬページは、ｄｒｍ　Ｗｅｂサービス１４が提供するセッション固有の一意のＵＲＬを特定するように再フォーマットされる。再フォーマットされたＨＴＭＬページは、ここでＷｅｂブラウザ１０に返される（矢印５）。

【００３５】次に、Ｗｅｂブラウザ１０はｄｒｍ　Ｗｅｂサービス１４内のクリアコンテンツ・キャッシュ２４にリダイレクタ・サービス・インターフェース２６を介して保存されるセキュアでないコンテンツを要求する（矢印６）。ブラウザの要求は、現在のブラウザ・セッションのみで有効なセッション固有のＵＲＬを含むクエリー・ストリングで構成される。リダイレクタ・サービス・インターフェイス２６は、現在のブラウザ・セッションを確認してブラウザ１０が送信するクエリー・ストリングに記述されるセッション固有のＵＲＬと比較する。セッションが一致し、クリア・コンテンツの一時記憶にタイムアウト規則があればその期限が切れていない場合に、リダイレクタ・サービス・インターフェイス２６はＷｅｂブラウザ１０にクリア・コンテンツを送信し、エンド・ユーザーはこれを利用できるようになる。

【００３６】本発明は、プロキシベースの介入とコンテンツの適応という新しい概念に基づいており、情報操作ポリシーとデジタル権利管理ポリシーの解釈と実施を総括するプラットフォームを提供する。これは、特にポータルなどの場合に有効である。このような状況では、ユーザーが様々な表示環境を使用する関連の大規模なベースに対して、一貫した柔軟な方法でポリシーを適用する必要がある。換言すれば、本発明を使用すると、組織の異機種ネットワーク上にユーザー固有の情報操作ポリシー（著作権行使のポリシーなど）を一貫して適用できる。

【００３７】本発明で採用する手法では、本質的にユーザー認証及び認可のプロセスとメカニズムをポリシー実施の実際の実装とは別に維持している。このことによって、組織又はコンテンツ・サービスは集中管理の企業データベースを利用して情報ポリシー（電子ジャーナルに

関する組織のサイト・ライセンスなど、特に組織内の様々なロールに様々なポリシーが適用される場合）を管理できる。

【００３８】明細書の以上の部分では、本発明についてその特定の典型的な実施態様に関連して記述してきた。ただし、前述の請求項に示す本発明の精神と範囲を逸脱しない限り、その様々な変形や変更が可能なことは、当業者には明らかである。従って、本明細書と図面は制限を意味するものではなく例示を意図するものと見なす必要がある。

【００３９】この発明は、例として次の実施形態を含む。

【００４０】（１）１つ又は複数のクライアント・プラットフォーム（１０）と１つ又は複数のリモート・プラットフォーム（１６）の間のプロキシ・サービス（１２）を提供する装置であって、（ａ）　リモート・プラットフォーム（１６）の電子的なコンテンツ又は情報に対するクライアント・プラットフォーム（１０）の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム（１６）に送信してデータを受け取る機能、または（ｂ）　前記リモート・プラットフォーム（１６）に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム（１０）から受け取る機能のいずれか又は両方を行う手段を備えており、前記データは要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス（１４）のロケーションを表す少なくとも１つのマーカーを含んでおり、前記装置は、前記１つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、（ａ）　前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能と、（ｂ）　前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、を備える前記装置。

【００４１】（２）プロキシ・サービス（１４）による情報又はコンテンツの要求に応答して１つ又は複数のマーカーを含むデータ・ストリームを返し、マーカーにはプロキシ・サービス（１２）がクライアント・プラットフォーム（１０）にコンテンツの複製を送信する前に対話する必要がある他の１つ又は複数のサービスのロケーションの詳細情報が含まれる（１）に記載の装置。

【００４２】（３）データ・ストリームにマーカーが埋め込まれており、プロキシ・サービス（１２）の内部で提供される専用の手段のみによってマーカーを認識でき、解釈できる（２）に記載の装置。

【００４３】（４）クライアント・プラットフォームがＷｅｂブラウザ（１０）などの場合、情報操作／権利管理リモート・サービス（１４）に情報又はコンテンツ要求を送信する際に、プロキシ・サービス（１２）が要求内にセッションＩＤなどのクライアント・プラットフォーム（１０）に関連するデータを含むように調整される（１）から（４）のいずれかに記載の装置。

【００４４】（５）情報操作／権利管理サービス（１４）がプロキシ・サービス（１２）からコンテンツ要求を受信して要求の合法性を検証すると、コンテンツのクリア・コンテンツ・バージョンを作成し、ローカル又はリモートの特定のロケーション（２４）に保存し、さらに前記ロケーションの詳細情報をプロキシ・サービス（１２）に返す（１）から（４）のいずれかに記載の装置。

【００４５】（６）前記コンテンツのクリア・コンテンツ・バージョンが一時的に記憶される（５）に記載の装置。

【００４６】（７）プロキシ・サービス（１２）がコンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォーム（１０）のロケーションの詳細情報を送信するように調整され、その結果、情報操作／権利管理サービス（１４）に関する特定の要件が満足された場合にクライアント・プラットフォーム（１０）が前記クリア・コンテンツの複製を取得できる（５）に記載の装置。

【００４７】（８）１つ又は複数のクライアント・プラットフォーム（１０）と１つ又は複数のリモート・プラットフォーム（１６）の間のプロキシ・サービス（１２）を提供する方法であって、（ａ）　リモート・プラットフォーム（１６）の電子的な情報又はコンテンツに対するクライアント・プラットフォーム（１０）の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム（１６）に送信してデータを受け取るステップと、（ｂ）　前記リモート・プラットフォーム（１６）に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム（１０）から受け取るステップのいずれか又は両方を含み、前記データに要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス（１４）のロケーションを表す少なくとも１つのマーカーが含まれており、さらに前記１つ又は複数のマーカーを解釈するステップと、情報操作／ポリシー実施のサービス（１２）の要件が満足された場合に、（ａ）前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォーム（１０）に提供するという要求を前記クライアント・プラットフォーム（１０）に代わって送信するステップと、（ｂ）　前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・プラットフォーム（１６）に提供するという要求を適切な情報操作ポリシー実施サービス（１２）に送信するステッ

13

プのいずれか又は両方を含む方法。

【図面の簡単な説明】

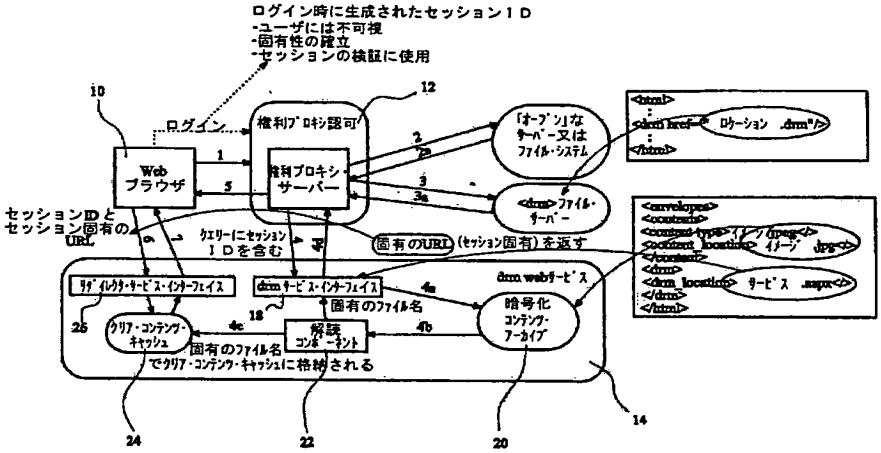
【図１】本発明の典型的な実施態様の動作の概略を表す流れ図である。

【符号の説明】

14

１０　クライアント・プラットフォーム
１２　プロキシ・サービス
１４　情報操作／権利管理リモート・サービス
１６　リモート・プラットフォーム

【図１】



フロントページの続き

(72)発明者　マーク・シュラゲター
アメリカ合衆国03054ニューハンプシャー
州メリマック、スコッチ・パイン　14

Ｆターム(参考)　5B017 AA07 BA06 CA16
5B085 AA08 AE02 AE23 BA07 BC02
BE04 BG04 BG07